

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-307043

(43)Date of publication of application : 02.11.2001

(51)Int.Cl.

G06K 19/07
G06F 9/06
G06F 12/14
G06K 19/073

(21)Application number : 2000-117323

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 19.04.2000

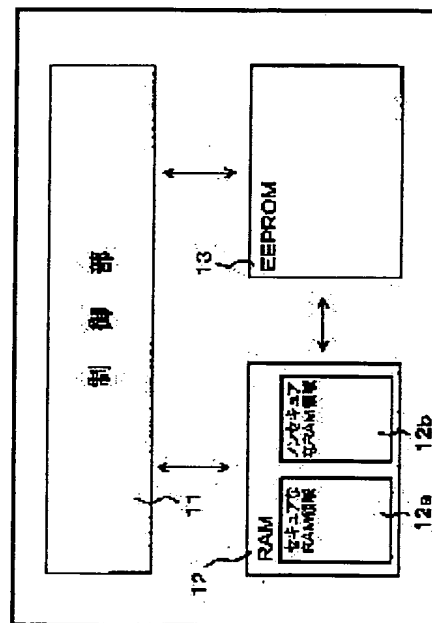
(72)Inventor : NOZAWA AKIO
KUNIMOTO SATOHARU
CHIKADA YASUYUKI

(54) MULTI-APPLICATION IC CARD AND ITS PROCESSING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a multi-application IC card with high security capable of shortening the processing time, and its processing method.

SOLUTION: This multi-application IC card is provided with a storage means 12 including a secured area 12a access to which is made impossible from the application after switching by resetting information application before the switching when plural applications are switched to be executed. It is provided with a confirming means 11 for confirming whether or not the security of the first application is satisfied, a setting means 12 for setting a security status in the secured area when the security is satisfied, a saving means 13 for saving the security status at switching from the first to the second application and a decoding means for decoding the saved security status at switching from the second to the first application.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-307043

(P2001-307043A)

(43) 公開日 平成13年11月2日 (2001. 11. 2)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコト* (参考)
G 0 6 K 19/07		G 0 6 F 9/06	5 5 0 A 5 B 0 1 7
G 0 6 F 9/06	5 5 0	12/14	3 1 0 J 5 B 0 3 5
12/14	3 1 0	G 0 6 K 19/00	N 5 B 0 7 6
G 0 6 K 19/073			P

審査請求 未請求 請求項の数 4 O L (全 7 頁)

(21) 出願番号 特願2000-117323 (P2000-117323)

(22) 出願日 平成12年4月19日 (2000. 4. 19)

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 野澤 昭雄

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

(72) 発明者 國本 聡治

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

(74) 代理人 100092576

弁理士 鎌田 久男

最終頁に続く

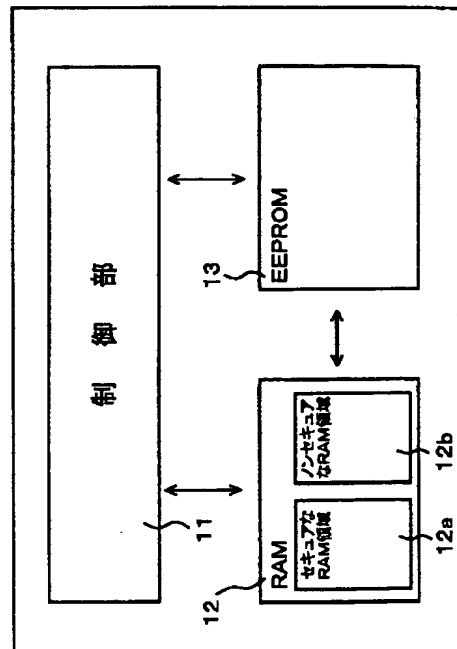
(54) 【発明の名称】 マルチアプリケーションICカード及びその処理方法

(57) 【要約】

【課題】 処理時間を短縮することができ、セキュリティ性の高いマルチアプリケーションICカード及びその処理方法を提供する。

【解決手段】 切り替えて実行する複数のアプリケーションの切替時に切替前のアプリケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域12aを含む記憶手段12を有するマルチアプリケーションICカードであって、第1のアプリケーションのセキュリティが満足できるか否かを確認する確認手段11と、セキュリティが満足できるときに、セキュリティステータスをセキュアな領域に設定する設定手段12と、第1から第2のアプリケーションへの切替時に、セキュリティステータスを退避させる退避手段13と、第2から第1のアプリケーションへの切替時に、退避したセキュリティステータスを復号させる復号化手段12とを備える。

101 →



【特許請求の範囲】

【請求項1】 切り替えて実行する複数のアプリケーションを有し、アプリケーション切替時に切替前のアプリケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域を含む記憶手段を有するマルチアプリケーションＩＣカードであって、

第1のアプリケーションのセキュリティが満足できるか否かを確認するセキュリティ確認手段と、

セキュリティが満足できるときに、セキュリティステータスを、前記セキュアな領域に設定するセキュリティステータス設定手段と、

前記第1のアプリケーションから第2のアプリケーションへの切替時に、前記セキュアな領域に設定されたセキュリティステータスを退避させるセキュリティステータス退避手段と、

前記第2のアプリケーションから前記第1のアプリケーションへの切替時に、前記セキュリティステータス退避手段に退避させられたセキュリティステータスを前記セキュアな領域に復号させるセキュリティステータス復号化手段とを備えるマルチアプリケーションＩＣカード。

【請求項2】 請求項1に記載のマルチアプリケーションＩＣカードにおいて、

前記記憶手段は、アプリケーション切替後も切替前の記憶を保持し、切替後のアプリケーションからもアクセス可能なノンセキュアな領域を含み、

前記セキュリティステータス退避手段に退避させられたセキュリティステータスの復号を許可するための暗号情報を作成して前記ノンセキュアな領域に保存する暗号保存手段と、

前記第1のアプリケーションから前記第2のアプリケーションに切り替えた後、再度、前記第1のアプリケーションに切り替えたときに、再度、暗号情報を作成し、その作成した暗号情報と、前記ノンセキュアな領域に保存されている暗号情報とを比較する暗号比較手段とを備え、

前記セキュリティステータス復号化手段は、前記暗号比較手段で比較した暗号情報が一致する場合に、前記退避させたセキュリティステータスを復号させることを特徴とするマルチアプリケーションＩＣカード。

【請求項3】 請求項2に記載のマルチアプリケーションＩＣカードにおいて、

前記暗号保存手段は、初めに、暗号を作成し、その作成した暗号を暗号化キーとして保存し、次に、その暗号化キーに基づいて暗号情報を作成し、

前記暗号比較手段は、前記暗号化キーに基づいて暗号情報を作成することを特徴とするマルチアプリケーションＩＣカード。

【請求項4】 切り替えて実行する複数のアプリケーションを有し、アプリケーション切替時に切替前のアプリ

ケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域及びアプリケーション切替後も切替前の記憶を保持し、切替後のアプリケーションからもアクセス可能なノンセキュアな領域を含む記憶手段を有するマルチアプリケーションＩＣカードの処理方法であって、

第1のアプリケーションのセキュリティが満足できるか否かを確認するセキュリティ確認工程と、

セキュリティが満足できるときに、セキュリティステータスを、前記セキュアな領域に設定するセキュリティステータス設定工程と、

前記第1のアプリケーションから第2のアプリケーションへの切替時に、前記セキュアな領域に設定されたセキュリティステータスを退避させるセキュリティステータス退避工程と、

暗号を作成し、その作成した暗号を暗号化キーとして保存し、次に、その暗号化キーに基づいて暗号情報を作成して前記ノンセキュアな領域に保存する暗号保存工程と、

前記第2のアプリケーションから前記第1のアプリケーションへの切替時に、再度、前記暗号化キーに基づいて暗号情報を作成し、その作成した暗号情報と、前記ノンセキュアな領域に保存されている暗号情報とを比較する暗号比較工程と、

前記暗号比較工程で比較した暗号情報が一致する場合に、前記退避させたセキュリティステータスを前記セキュアな領域に復号させるセキュリティステータス復号化工程とを備えるマルチアプリケーションＩＣカードの処理方法。

30 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数のアプリケーションを切り替えて使用するマルチアプリケーションＩＣカード及びその処理方法に関するものである。

【0002】

【従来の技術】従来、ＩＣカードは、例えば、信販会社のクレジットカードのように、一企業から発行され、その企業の単一アプリケーションのみ組み込まれ、単一機能のみ果たすものが多かった。そのようなＩＣカードでは、図5に示すように、まず、暗証番号等を照合（VERIFY）し（ステップ（以下「S」という。）310）、セキュリティが満足されていることが確認できたときは、セキュリティステータス（Security Status（SS））が設定され（S320）、処理コマンド（例えば、READ RECORD）が実行される（S330）。ところが、最近では、例えば、信販会社のクレジットカード機能と、家電量販店のポイントカード機能というように、複数企業のアプリケーションが1枚のカードに組み込まれた、いわゆるマルチアプリケーションＩＣカードが普及しつつある。このようなI

40

Cカードによれば、例えば、家電量販店での買い物に、まず、家電量販店のポイントで支払い、不足分をクレジットカードで支払うことを、1枚のICカードで済ませることができる。

【0003】

【発明が解決しようとする課題】しかし、クレジットカード兼ポイントカードのようなマルチアプリケーションICカードの場合は、例えば、ポイントカードについてのセキュリティステータス(SS)に基づいて、クレジットカードの処理が行われたりすることのないように、アプリケーションが切り替わると、前のアプリケーションのセキュリティステータス(SS)は、リセットされる。そのため、図6に示すように、初めのVERIFY(S410)に基づいて、ポイントカードのセキュリティステータス(SS)が設定されるが(S420)、続いて、クレジットカードのアプリケーションが選択(SELECT)され(S430)、クレジットカードのセキュリティステータス(SS)が設定されると、元のポイントカードのセキュリティステータス(SS)がリセットされるので(S440)、再度、ポイントカードのREAD RECORDコマンド処理することができず(S450)、エラー(ERR)になる(S460)。したがって、このような場合は、ポイント支払い時、クレジット支払い時、クレジット支払いに基づく新たなポイント加算時と、3回、図5に示す処理を繰り返さなければならない場合があるなど、処理時間が、かかっている。

【0004】本発明の課題は、処理時間を短縮することができ、セキュリティ性の高いマルチアプリケーションICカード及びその処理方法を提供することである。

【0005】

【課題を解決するための手段】本発明は、以下のような解決手段により、前記課題を解決する。なお、理解を容易にするために、本発明の実施形態に対応する符号を付して説明するが、これに限定されるものではない。前記課題を解決するために、請求項1の発明は、切り替えて実行する複数のアプリケーションを有し、アプリケーション切替時に切替前のアプリケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域(12a)を含む記憶手段(12)を有するマルチアプリケーションICカードであって、第1のアプリケーションのセキュリティが満足できるか否かを確認するセキュリティ確認手段(11)と、セキュリティが満足できるときに、セキュリティステータスを、前記セキュアな領域(12a)に設定するセキュリティステータス設定手段(12)と、前記第1のアプリケーションから第2のアプリケーションへの切替時に、前記セキュアな領域(12a)に設定されたセキュリティステータスを退避させるセキュリティステータス退避手段

(13)と、前記第2のアプリケーションから前記第1のアプリケーションへの切替時に、前記セキュリティステータス退避手段(13)に退避させられたセキュリティステータスを前記セキュアな領域(12a)に復号させるセキュリティステータス復号化手段(12)とを備えるマルチアプリケーションICカードである。

【0006】請求項2の発明は、請求項1に記載のマルチアプリケーションICカードにおいて、前記記憶手段(12)は、アプリケーション切替後も切替前の記憶を保持し、切替後のアプリケーションからもアクセス可能なノンセキュアな領域(12b)を含み、前記セキュリティステータス退避手段(13)に退避させられたセキュリティステータスの復号を許可するための暗号情報を作成して前記ノンセキュアな領域(12b)に保存する暗号保存手段(12)と、前記第1のアプリケーションから前記第2のアプリケーションに切り替えた後、再度、前記第1のアプリケーションに切り替えたときに、再度、暗号情報を作成し、その作成した暗号情報と、前記ノンセキュアな領域(12b)に保存されている暗号情報とを比較する暗号比較手段(11)とを備え、前記セキュリティステータス復号化手段(12)は、前記暗号比較手段(11)で比較した暗号情報が一致する場合に、前記退避させたセキュリティステータスを復号させることを特徴とするマルチアプリケーションICカードである。

【0007】請求項3の発明は、請求項2に記載のマルチアプリケーションICカードにおいて、前記暗号保存手段(12)は、初めに、暗号を作成し、その作成した暗号を暗号化キーとして保存し、次に、その暗号化キーに基づいて暗号情報を作成し、前記暗号比較手段(11)は、前記暗号化キーに基づいて暗号情報を作成することを特徴とするマルチアプリケーションICカードである。

【0008】請求項4の発明は、切り替えて実行する複数のアプリケーションを有し、アプリケーション切替時に切替前のアプリケーションの情報をリセットして切替後のアプリケーションからはアクセス不能なセキュアな領域(12a)及びアプリケーション切替後も切替前の記憶を保持し、切替後のアプリケーションからもアクセス可能なノンセキュアな領域(12b)を含む記憶手段(12)を有するマルチアプリケーションICカードの処理方法であって、第1のアプリケーションのセキュリティが満足できるか否かを確認するセキュリティ確認工程(S110)と、セキュリティが満足できるときに、セキュリティステータスを、前記セキュアな領域(12a)に設定するセキュリティステータス設定工程(S120)と、前記第1のアプリケーションから第2のアプリケーションへの切替時に、前記セキュアな領域(12a)に設定されたセキュリティステータスを退避させるセキュリティステータス退避工程(S122)と、暗号

を作成し、その作成した暗号を暗号化キーとして保存し、次に、その暗号化キーに基づいて暗号情報を作成して前記ノンセキュアな領域(12b)に保存する暗号保存工程(S125)と、前記第2のアプリケーションから前記第1のアプリケーションへの切替時に、再度、前記暗号化キーに基づいて暗号情報を作成し、その作成した暗号情報と、前記ノンセキュアな領域(12b)に保存されている暗号情報とを比較する暗号比較工程(S160)と、前記暗号比較工程(S160)で比較した暗号情報が一致する場合に、前記退避させたセキュリティステータスを前記セキュアな領域(12a)に復号させるセキュリティステータス復号化工程(S170)とを備えるマルチアプリケーションICカードの処理方法である。

【0009】

【発明の実施の形態】以下、図面等を参照して、本発明の実施の形態について、さらに詳しく説明する。図1は、本発明によるマルチアプリケーションICカードの実施形態を示すブロック図である。マルチアプリケーションICカード10は、制御部11と、RAM12と、EEPROM13とを備える。

【0010】制御部11は、本マルチアプリケーションICカード10全体の制御を行う部分である。RAM12は、セキュリティステータス(SS)等のデータを記憶する揮発性メモリであり、Dynamicである。RAM12は、セキュアなRAM領域12aと、ノンセキュアなRAM領域12bとを有する。セキュアなRAM領域12aは、アプリケーションを切り替えると、セキュリティ保持のために切替前の記憶をリセットし、切替後のアプリケーションからはアクセスできない領域である。ノンセキュアなRAM領域12bは、アプリケーションを切り替えても、切替前の記憶を保持しておき、切替後のアプリケーションや外部からアクセス可能な領域であり、Publicである。

【0011】EEPROM13は、Random Number Seed、Dupliated SS、Static Session Key等のデータを記憶する不揮発性メモリであり、Staticである。Random Number Seedは、乱数を発生させる際の、いわゆる種となるデータである。Random Number Seedは、8バイトのデータであり、初期値は、00000000000000000000hである。Dupliated SSは、セキュリティステータス(SS)を複製したデータであり、後述のように、セキュリティステータス(SS)を復元する際の際となるデータである。Dupliated SSは、1バイトのデータであり、初期値は、00hである。Static Session Keyは、Random Number Seedを暗号化する際の鍵となるデータである。Static Session Keyは、8

バイトのデータであり、初期値は、00000000000000000000hである。

【0012】図2は、本発明の実施形態に係るマルチアプリケーションICカードの動作を説明するフローチャートである。制御部11の動作を中心として、マルチアプリケーションICカード10の動作を説明する。制御部11は、暗証番号等の照合(VERIFY)を行い(S110)、セキュリティが満足できれば、セキュリティステータス(SS)の設定を行う(S120)。制御部11は、別のアプリケーションを選択するSELECTコマンドを受信して(S130)、そのアプリケーションを実行(Load)した後(S140)、再度、元のアプリケーションを選択するSELECTコマンドを受信したら(S150)、認証コードチェックを行う(S160)。認証コードが正しいときは、制御部11は、EEPROM13に複製しておいたセキュリティステータス(Dupliated SS)を復号化して(S170)、セキュアなRAM領域12aに書き込み(S180)、READ RECORDコマンドを実行する(S190)。一方、認証コードが正しくないときは、制御部11は、再度、セキュリティが満足できるかを照合(VERIFY)し(S200)、セキュリティが満足できれば、セキュリティステータス(SS)の設定を行った後(S210)、READ RECORDコマンドを実行する(S190)。

【0013】図3は、セキュリティステータスの設定動作の詳細について説明するフローチャートである。VERIFYの結果、セキュリティが満足できるときは、制御部11は、セキュアなRAM領域12aにセキュリティステータス(SS)をセットする(S121)。そして、制御部11は、そのセットしたセキュリティステータス(SS)を、EEPROM13にDupliated SSとしてコピーする(S122)。続いて、制御部11は、乱数を生成して、その生成した乱数をEEPROM13にRandom Number Seedとして保存し(S123)、また、このRandom Number Seedを、EEPROM13に予め設定してあるStatic Session Keyをキーとして、ECB DES暗号化し、暗号化結果を新たなStatic Session KeyとしてEEPROM13に保存する(S124)。さらに、制御部11は、Random Number Seedを、S124において生成したStatic Session Keyをキーとして、再度、ECB DES暗号化して、その暗号化結果を、今度は、ノンセキュアなRAM領域12bのEnciphered Random Numberとして格納する(S125)。

【0014】図4は、認証コードチェック動作の詳細について説明するフローチャートである。制御部11は、EEPROM13に保存されているRandom Nu

umber Seed及びStatic Session Keyを読み出し(S161)、Static Session Keyをキーとして、Random Number Seedを、ECB DES暗号化して(S162)、その暗号化結果と、ノンセキュアなRAM領域12bのEnciphered Random Numberとを比較する(S163)。その結果、両者が同一のときは、図2に示すように、EEPROM13のDuplicated SSを、セキュアなRAM領域12aにセキュリティステータス(SS)としてコピーして復号化するが(S170)、両者が同一でないときは、復号化せず、再度、VERIFYする(S200)。

【0015】本実施形態によれば、一旦、確認したセキュリティステータス(SS)を保存するので、再度、VERIFYする必要がなく、処理速度を短縮化することができる。また、毎回、Static Session Keyを変更して保存するので、毎回、暗号が変わり、セキュリティ性が高い。

【0016】(変形形態)以上説明した実施形態に限定されることなく、種々の変形や変更が可能であって、それらも本発明の均等の範囲内である。例えば、暗号化方法としては、ECB DES暗号に限らず、他の公知の方法で暗号化しても、同様の効果が得られる。

【0017】

【発明の効果】以上詳しく説明したように、請求項1の発明によれば、第1のアプリケーションから第2のアプリケーションへの切替時に、第1のアプリケーションのセキュリティステータスを退避させ、第2のアプリケーションから第1のアプリケーションへの切替時に、その退避させたセキュリティステータスを復号させるので、再度、VERIFYする必要がなく、処理速度を短縮化することができる。

【0018】請求項2の発明によれば、セキュリティステータスの復号を許可するための暗号情報をノンセキュアな領域に保存し、第1のアプリケーションから第2の

アプリケーションに切り替えた後、再度、第1のアプリケーションに切り替えたときに、再度、暗号情報を作成して、両暗号を比較して、セキュリティステータスを復号化するので、セキュリティ性が高い。

【0019】請求項3の発明によれば、暗号化キーを作成して、その暗号化キーに基づいて暗号情報を作成するので、毎回、暗号が変わり、セキュリティ性が高い。

【0020】請求項4の発明によれば、第1のアプリケーションから第2のアプリケーションへの切替時に、第1のアプリケーションのセキュリティステータスを退避させ、第2のアプリケーションから第1のアプリケーションへの切替時に、暗号に基づいて、その退避させたセキュリティステータスを復号させるので、再度、VERIFYする必要がなく、処理速度を短縮化することができる。また、セキュリティ性が高い。

【図面の簡単な説明】

【図1】本発明によるマルチアプリケーションICカードの実施形態を示すブロック図である。

【図2】本発明の実施形態に係るマルチアプリケーションICカードの動作を説明するフローチャートである。

【図3】セキュリティステータスの設定動作の詳細について説明するフローチャートである。

【図4】認証コードチェック動作の詳細について説明するフローチャートである。

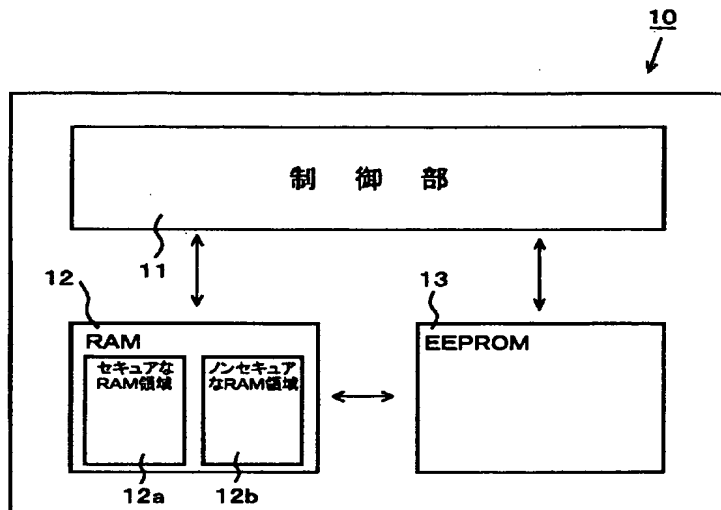
【図5】従来の単一機能ICカードの動作を説明するフローチャートである。

【図6】マルチアプリケーションICカードの動作を説明するフローチャートである。

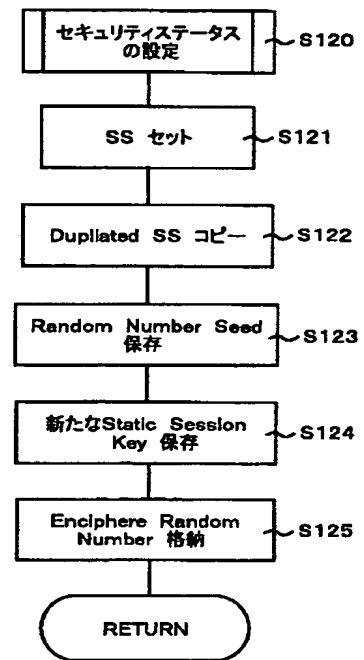
【符号の説明】

- 10 マルチアプリケーションICカード
- 11 制御部
- 12 RAM
- 12a セキュアなRAM領域
- 12b ノンセキュアなRAM領域
- 13 EEPROM

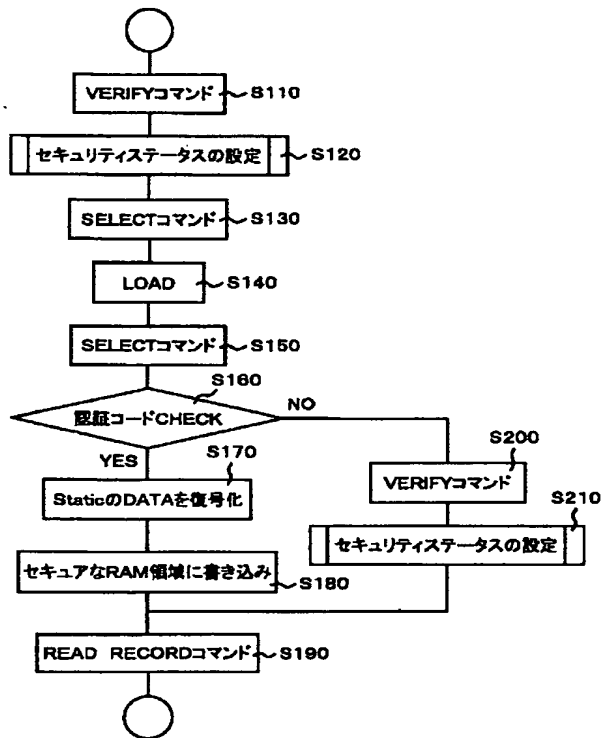
【図1】



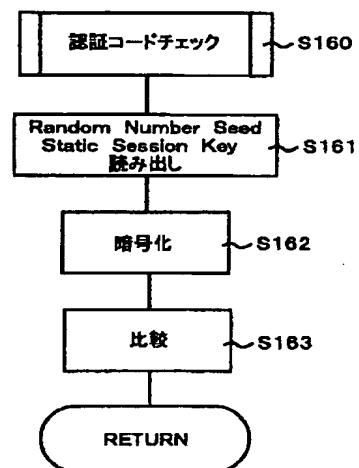
【図3】



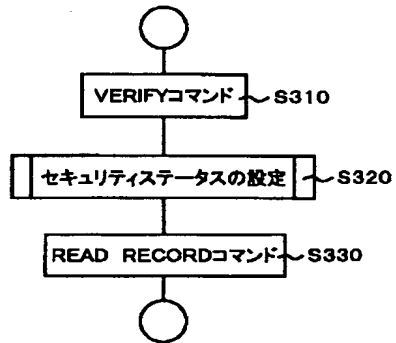
【図2】



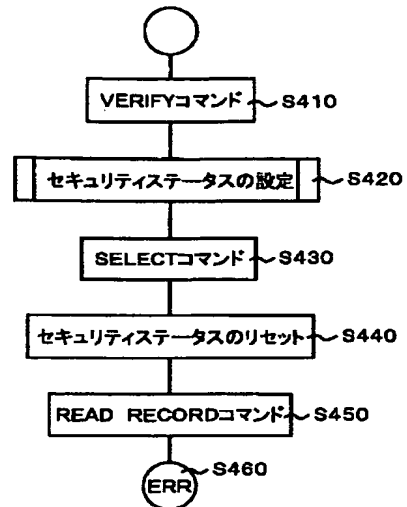
【図4】



【図5】



【図6】



フロントページの続き

(72)発明者 近田 恭之
 東京都新宿区市谷加賀町一丁目1番1号
 大日本印刷株式会社内

Fターム(参考) 5B017 AA07 BA02 BB09 CA14
 5B035 AA06 BB09 BC00 CA39
 5B076 AB17 FB01